Prof. Philip Koopman

Carnegie Mellon University

@PhilKoopman

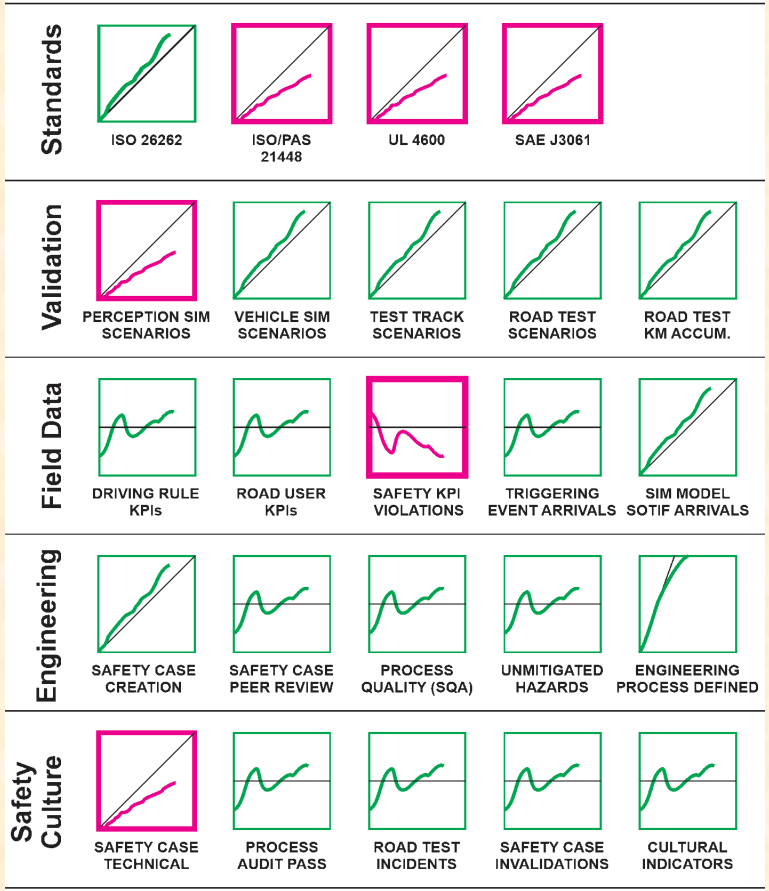
EDGE CASE RESEARCH

Safety Cases & Highly Automated Vehicle Safety

September 2020

Overview

- Important to know when a self-driving car design is acceptably safe
  - What do we measure?
- Safety case ties together:
  - Standards-based engineering
  - Knowing what to measure
  - Showing that system is acceptably safe



Hypothetical Dashboard

Standards-Based Engineering Approach

EDGE CASE RESEARCH

SYSTEM SAFETY	UL 4600		**Safety Beyond Dynamic Driving**
DYNAMIC DRIVING FUNCTION	ISO/PAS 21448	SaFAD/ISO TR 4804	**Environment & Edge Cases**
FUNCTIONAL SAFETY	ISO 26262		**Equipment Faults**
CYBER-SECURITY	SAE J3061	SAE 21434	**Computer Security**
VEHICLE SAFETY	FMVSS	NCAP	**Basic Vehicle Functions**

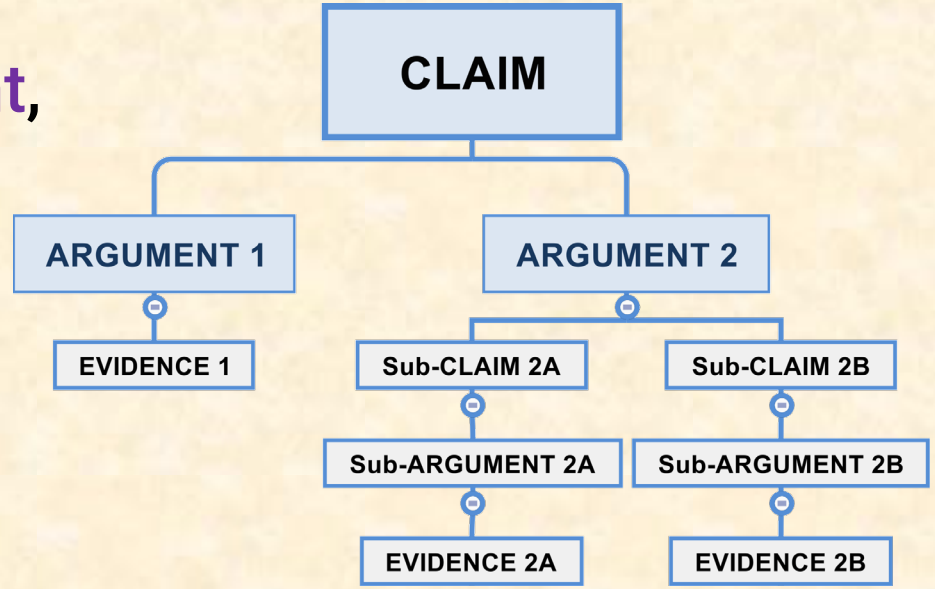
HIGHLY AUTOMATED VEHICLE SAFETY CASE

UL 4600

Explaining Via A Safety Case

EDGE CASE RESEARCH

- **Safety Case:**
  A structured written argument, supported by evidence, justifying system is acceptably safe for intended use.



- **Answers questions:**
  - What do you mean by “safe” (claim)
  - Explain why you think you’re safe (argument)
  - Show data to support your explanation (evidence)

From Safety Case To Dashboard

EDGE CASE RESEARCH

- Safety Performance Indicators (SPIs) for safety case claims
  - Standards: Cover relevant standards, best practices
  - Validation: Safety metrics from testing predict acceptable risk
  - Process: Engineering rigor and process quality metrics
  - Feedback: Field feedback data shows risk prediction is accurate
  - Safety Culture: Metrics indicate a healthy safety culture
- Dashboard:
  - Deploy when SPIs show your claims are supported by data

EDGE CASE RESEARCH

WE DELIVER THE PROMISE OF AUTONOMY